Cybersecurity Issues of Intelligent Power Supply Systems for Electricity Consumers

Belov S.I.[1][a] and Pushkareva M.B.[2][b]
[1]*Department of power supply and electric machines, National Research University, Russian State Agrarian University Moscow, Russia*
[2]*Department of Management and marketing of high-tech industries, National Research University Moscow Aviation Institute, Moscow, Russia*
sbelov_@mail.ru, *mpushkareva@narod.ru*

Keywords: Cybersecurity, Digital energy, Internet of energy, Distributed energy, Load management, Micro-energy system, SmartGrid.

Abstract: The paper discusses the issues of cybersecurity of intelligent end-user control systems at the stage of development of digital energy management platforms in the retail electricity market. The analysis of the process of development of energy supply to consumers and the transition to distributed electric power platforms in which the information and control subsystem is comparable in complexity and responsibility with the physical one, which accordingly requires ensuring safe operation and uninterrupted supply of consumers, especially in the conditions of import substitution. At the moment, the problem of cybersecurity of digital energy is a key one and in the future this role will only increase.

1 INTRODUCTION

The fundamental document for the development of domestic energy is the Energy Strategy of the Russian Federation for the period up to 2035, as a result of which sustainable, reliable and effective satisfaction of domestic demand for energy resources and services in the energy sector, as well as the energy security of the country and ensuring anti-terrorist protection of equipment and information infrastructure of fuel and energy complex facilities should be ensured (Energeticheskaya strategiya Rossijskoj Federacii na period do 2035 goda).

At the same time, the Energy Strategy of the Russian Federation particularly notes that at present, processes are taking place in the global energy sector, including the Russian one, which at the turn of the 30 - 40s of the XXI century will lead to a change in the established way of life, especially in the traditionally centralized power supply system: carbon energy will be supplemented by renewable energy sources, centralized energy supply - decentralized, the range of electric energy applications will significantly expand, domestic technologies, equipment and services in the energy sector will be actively introduced, the processes of digital transformation and intellectualization of accounting, analysis and management of processes of generation, transmission and consumption of electricity will be consistently developed, new rights and opportunities will be given to end-users of energy resources for the introduction of new digital technologies for the analysis of operating modes in real-time process and self-load management.

The processes of increasing activity of consumers in managing their energy consumption based on energy efficiency, reducing greenhouse emissions and using renewable energy sources, ensuring energy independence of the end-user, the development of small distributed generation and decentralization of energy supply, the transition to information and telecommunication technologies and intelligent management are a serious challenge in the energy sector.

Distributed (small) sources of energy generation fundamentally change the architecture and principles of building power systems, the use of intelligent

[a] https://orcid.org/0000-0003-3974-6734
[b] https://orcid.org/0000-0002-7600-0336

forecasting for automated control of modes makes it possible to increase the accuracy of their planning, reduce the power deficit, reduce the financial burden on consumers, minimize human participation in this process.

The primary source of information in the vast majority of cases are modern intelligent metering systems for electrical and thermal energy, which allow not only to collect information at the pace of the process, but also to form a certain set of control actions. This factor becomes significant not only for the electric grid complex, it affects gas, oil and heat supply systems (Stennikov, 2023).

The processes of digitalization of the Russian electric power industry at all levels from generation to the end-user (including the population) require fundamental changes in the entire information infrastructure of fuel and energy complex facilities.

Electrification is recognized as the greatest achievement in terms of its impact on the quality of life and as a unique critical system on which the energy supply of consumers with all types of energy resources, including water supply, depends to a great extent.

The gradual transformation of the established way of the traditional centralized system of electric power industry as a result of the transition to information and telecommunication technologies and intelligent management of energy resources due to the formation of intelligent networks and an active consumer of electricity leads to the formation of a huge flow of information and mutual exchange of information between an ever-increasing large number of end active consumers of electricity with various technologies and modes of operation.

Smart grids carry not only great advantages for the consumer, but also disadvantages, when neglecting security issues can eventually endanger, for example, the supply of electricity, water, or gas, and public infrastructure, government agencies or citizens may be threatened or become the object of manipulation. Therefore, the process of developing smart networks should be carried out in parallel with the development of protocols that reliably preserve the confidentiality of customers in smart network scenarios, underlie secure, verifiable, efficient and scalable programs with low communication overhead and resistant to unauthorized external penetration.

2 TASKS AND OPPORTUNITIES FOR THE DEVELOPMENT OF INTELLIGENT POWER SUPPLY SYSTEMS FOR CONSUMERS IN RUSSIA

Modern generating stations of small and medium capacity have become sufficiently cheap, reliable, technological and efficient so that their own generation on their basis successfully competes with the purchase of electricity from the grid. Managing the load of own energy facilities with the help of digital intelligent systems will make it possible to extract even greater economic benefits without attracting highly qualified specialized personnel on a permanent basis. A new format of relations between a retail producer and industrial consumers of electric energy is emerging, requiring structural transformations of energy systems and changes in the basic provisions of the functioning of retail electricity markets.

Decree of the Government of the Russian Federation No. 320 dated 21.03.2020 "On Amendments to Certain Acts of the Government of the Russian Federation on the Functioning of Active Energy Complexes" provided the opportunity to launch pilot projects for the organization of microgrids by industrial and commercial consumers (the official term used is active energy complex - AEC), where energy receiving devices of industrial enterprises, administrative and business, sports and entertainment cultural centers with the use of innovative technologies and managed intelligent connections can be combined in order to increase energy saving and reduce the financial burden for energy resources, leading to lower costs for all consumers.

The potential of the Russian market of commercial and industrial microgrids will reach 1.2 GW per year of installed capacity by 2028. The realization of this potential will allow the Russian economy, according to an approximate estimate, to get an economic effect of up to 150 billion rubles in 2020-2028, minus investments in microgrids (Aktivnye energeticheskie kompleksy — pervyj shag k promyshlennym mikrogridam v Rossii).

The new business practice of creating and ensuring the functioning of microgrids for industrial and commercial consumers creates new opportunities not only for the organizers and users of this practice, but also for developers of new technologies and suppliers of technological solutions for microgrids.

Digital technologies are being rapidly developed and implemented, which include the Internet of Things, 3D modeling, modeling and forecasting based on the analysis of Big Data, intelligent electrical networks (Smart Grids), intelligent sensors and meters, neural networks, cloud and fog computing, creating virtual and augmented reality, computer simulation based on digital doubles, production robotics and additive technologies. All these technologies are beginning to be actively implemented at the level of the end-user of energy resources to optimize energy consumption management to improve energy efficiency and save energy resources.

In the energy policy of Russia, there is a progressive movement towards the development of the retail segment of the electric power industry based on the principles of the Internet of Energy as an ecosystem of energy producers and consumers, where a fundamentally new model of free exchange of energy resources and services by market participants appears instead of the traditional "production-distribution-sales-consumption" system.

Digital transformation of the energy sector allows, on the basis of integrated industry digital platforms of a new generation, to ensure equal access of mass ordinary participants of the retail energy market to the full range of opportunities and functions of energy entities. Each owner of even a small capacity of generating equipment has the opportunity not only to consume energy resources supplied by authorized operators of centralized power systems, but also to independently generate, store and transfer part of their own energy resources to the common network (Holkin, 2021).

Modern digital technologies, thanks to their high speed, make it possible to monitor changing processes in the operation of various equipment and technological processes in almost real time, present this work in a form convenient for quick analysis, predict the load, respond in a timely manner to critical deviations from normal operation and automatically control the operating modes of various equipment.

With the development of distributed generation, with the appearance of an increasing number of consumers in industry and up to the level of households, allowing them to actively change the usual load profiles, digital models for forecasting and managing energy consumption are becoming more complex.

The improvement of energy-efficient and digital technologies leads to a large-scale change in the technological structure in the energy sector, inevitably changes the appearance of all existing energy systems in the world and forms new principles of their management. There is a gradual integration of electric, heat, gas, and cold supply systems into a single energy ecosystem based on innovative technologies and the intellectualization of energy consumption. The increasing role of consumers in energy consumption management, the use of their own generation sources and alternative energy sources, the use of smart grids, the joint production of electricity, heat and cold at the generation level and the integration of consumers into a microsystem with the integration of end-user energy supply systems into a single energy power system requires a revision of the principles of construction, functioning and development of energy systems. Digitalization of integrated energy systems and their intellectualization cover a wide range of issues, including technical, organizational, regulatory, economic and others.

The development of energy and, especially, the electric power industry in the XXI century is proceeding at such a rapid and revolutionary pace that, accordingly, requires completely new approaches and knowledge in managing these processes, including energy resource consumption management in order to increase the energy efficiency of all end-users: from large enterprises to small organizations, the population and households.

In the conditions of decentralization of the architecture of power systems, it becomes possible for a huge number of distributed consumers to work together, while the complexity of managing the digital and technological base of a large number of participants increases with the number of participants in interaction. Users of such a system can be owners of any generating, accumulating and consuming energy equipment (industrial, commercial, household) having a common point of connection to energy networks and information channels, integrate into the system through interfaces and become full-fledged participants in new services and business models of the Internet of energy, providing services to each other, for example, such as supply of electrical energy.

Small generation, energy storage systems, regulated load of end-users, integrated with each other and with a centralized power system, represent a resource that has not yet been used to improve the efficiency of power systems. Distributed energy increases the efficiency of the power system by reducing the need for connected power, the emergence of local self-balancing associations of generators and low-power consumers, large-scale involvement of a mass of small but numerous energy assets of end-users in the management processes of the power system. An energy system with the ability to integrate new users and decentralize the management of a large number of distributed energy facilities will play a crucial role in the development of the electric power industry in the near future (Hohlov, 2018).

The development of intelligent power supply systems for consumers and the transition to distributed electric power platforms through the introduction of SmartGrid technologies (Suhov, Stushkina, 2021), the modernization of power supply systems by installing solar power plants or other sources of low-power self-generation on the consumer side requires ensuring appropriate indicators of electricity quality and reliability in power supply systems (Leshtaev, Stushkina, Zaginajlov, 2021), the need to resist physical and informational negative impacts without total shutdowns or high costs for restoration work require a corresponding increase in the manageability of both individual elements and the micro-energy system as a whole by creating digital platforms for multilateral communications and energy-information links for effective management and financial settlements, taking into account the entire variety of types of consumers and power plants installed on the consumer side.

Management of such a complex power supply system for an active consumer is impossible without creating an appropriate infrastructure of smart meters and an automatic power management system, which should become an information conductor for each consumer entering the micro-energy system with both market and technical operators of the electric power market. A general set of guidelines for the implementation of intelligent energy systems is presented by the IEC in the Smart Grid standardization roadmap and covers the improvement of the electric grid using intelligent technologies to solve pressing problems of improving the efficiency, reliability, observability and manageability of the power system and connected consumers, for the benefit of all stakeholders (IEC TR 62746-2; IEC TR 63097).

The open architecture of the Smart Grid software simplifies the management of business processes and consumer equipment: billing, financial calculations, planning, engineering and technological systems, etc. Solutions at the present stage are built on standard communication protocols to ensure compatibility with metering devices and systems from different manufacturers, open communication standards are applied that provide flexibility in their use, and the infrastructure itself is an integrated system of smart meters, communication networks and data management systems that provides two-way communication between consumers and energy suppliers. The system provides a number of important functions that were previously impossible or had to be performed manually, for example, the ability to automatically and remotely measure electricity consumption, connect and disconnect services, detect unauthorized interference, use new time-bound tariff plans and incentives to reduce peak demand and manage energy consumption.

The consumer can now manage their own energy consumption in real time and receive information about how and how much the subscriber spends on energy resources, in a visual form encouraging them to take actions to optimize their costs.

For an energy supply organization, this provides an increase in operational efficiency, an increase in network reliability and electricity quality, allows optimizing investments in infrastructure and improves the quality of customer service. The consumer, in turn, gets the opportunity to use energy rationally and improve energy efficiency, implement solutions for forecasting and notifying about energy consumption for adaptive automation of technological processes and learning how to manage these processes without user participation. Intelligent power management monitoring systems are already available and are used in large commercial buildings and industrial facilities in Russia and abroad (Mishuchkov, Pushkareva, Belov, 2020).

3 DEVELOPMENT OF INTELLIGENT MARKET MODELS IN THE CONDITIONS OF THE EMERGENCE OF ACTIVE ELECTRICITY CONSUMERS

In future distributed power systems, the information and communication component of power equipment management processes is becoming increasingly complex and responsible from the point of view of ensuring normal functioning and increasing consumer requirements for the reliability of their power supply and the quality of electricity supplied to them. In the conditions of digitalization, such an energy system increasingly needs to be considered as a complex cyber-physical complex with new properties and escalating problems of reliability and cybersecurity.

In this direction, it is necessary to conduct comprehensive research, the recommendations of which will ensure the necessary level of cybersecurity of digital intelligent power systems. Multiple examples of real situations of cyberattacks on electric power facilities of industrial enterprises, substations, power plants and analysis of the results in terms of forming scenarios of potentially possible cyberattacks to identify vulnerabilities and develop cyber-physical models of the power system to study the consequences of cyberattacks to justify measures to counter cyber threats and reduce negative consequences as a result of their possible implementation are given in (Voropaj, Kolosok, Korkina, Osak, 2019).

A lot of new generation consumers are constantly growing and developing with the use of modern technologies and electrical equipment with intelligent properties, using their own generation facilities, renewable energy sources and energy storage systems. These are high-tech and robotic enterprises, life support systems, energy-efficient buildings, data processing centers (data centers) and other consumers requiring special conditions for reliability and quality of power supply.

The driver of this development is not only the growing demand for electric energy and energy supply reliability indicators, but also progress in a number of energy and information and communication technologies, including those based on wireless communications, the rapid development of the Internet and applications based on it, cloud technologies and fog computing, big data processing, distributed control systems, the desire and ability of all participants in the power supply, and consumers in the first place, to benefit from the synergetic effect created by new technologies.

Due to the intensive development of distributed generation and automatically controlled electrical equipment on the consumer side, the volumes of generation facilities involved in management can be very serious, and the number of active consumers themselves and controlled equipment on their side with a variety of consumer types, their properties and requests can exceed the scale of management in the traditional electric power industry by orders of magnitude.

The power supply of active consumers should be provided with an infrastructure of intelligent measurements with intelligent sensors and meters for monitoring commercial and technological electricity consumption for energy-efficient management of own energy consumption and real-time settlements for received or given electricity between other participants of the local retail energy market.

These devices, in addition to building an intelligent demand management system, can provide control over the reliability of power supply, the quality of electrical energy and are an interface for communication with the aggregator and the existing market operator at the top level for the integration of distributed generation of various types into the public network.

In accordance with the business model, the AEC aggregator should collect the capacity of all consumers and use very advanced and new billing settlement technologies, smart contracts and distributed ledger technologies to settle accounts with the client. Such participation takes place in real time, requires automatic registration of the transaction and the development of a universal communication system from household networks to top-level dispatch control centers based on unified data models.

An extremely critical moment for a micro-energy system saturated with various electrical equipment and a digital product is the dependence of the reliability of such a system on the public network. A sudden disruption of external power supply, if distributed self-generating facilities cannot instantly provide sufficient power for reliable power supply to consumers of the micro-energy system, can lead to a local collapse: the loss of not only power supply, but also water supply, heat supply, gas supply, as well as the Internet.

On the other hand, sudden disruptions within the micro-energy system can affect the stability and reliability of the top-level power system to which the AEC is connected. The practice of technological/regime/emergency management in the power system is such that the end-user has always been considered as a passive element subordinate to system tasks. The system of automatic monitoring and control by the system and market operators of the power system does not reach the level of the average voltage of the end-user, while the distribution networks of medium voltage are designed and operated for radial operation and do not assume receiving power from the end-user. The existing means of communication of system operators are completely insufficient for their adjustment to new objects and tasks of active consumer technologies.

Thus, for the existing control system in the electric power industry, in technological and market/trade aspects, the solution of these tasks starts from scratch.

Effective use of the resources of an active consumer requires the development of market models, the sphere of system services, including the pricing process in the retail market in real time, the building of an integrated demand management system and the cardinal development of digital management platforms of technological and information platforms for reliable interaction of numerous participants in the system of active energy consumption in the retail market.

4 CYBERSECURITY ISSUES IN CONNECTION WITH THE DEVELOPMENT OF INTELLIGENT POWER SUPPLY SYSTEMS FOR THE END-USER

Cybersecurity issues in connection with the spread of the concept of intelligent power supply systems in the retail electricity market should be considered in relation to the energy security of Russia, since energy is connected with all industries and largely ensures their functioning. The increasing threats to cybersecurity due to the development of intelligent energy systems and the increase in the level of computerization and intellectualization of energy should be considered as one of the most important modern threats to Russia's energy security.

The increased complexity of the information network increases the number of vulnerabilities for potential attacks and unintended errors. Networks interconnected with other networks, which can also occupy several smart network domains, increase the likelihood of cascading accidents. A large number of interconnections of software components increases the vulnerability of the program code, which makes it easier for attackers to introduce malicious code and vulnerabilities into the program code. As the network nodes increase, the number of entry points for intruders also increases.

There is still no clear understanding of cybersecurity in Russia. It is often considered synonymous with information security or its component, which is why cybersecurity is not given enough attention. It is advisable to consider cybersecurity as a result of the convergence of five main components: application security, information security, network security, Internet application security, protection of key information systems of critical infrastructure facilities.

The introduction of modern information technologies and the increase in the level of intelligence of energy systems exacerbates the problem of cybersecurity, and, accordingly, energy security

Among these threats, cybersecurity threats have not been considered until recently, the implementation of which can provoke the most serious emergencies in the energy sector, fraught with a significant reduction in the ability to provide consumers with energy resources.

For example, in the case of a successful attack by cybercriminals on computers that control the operation of the power system, local accidents can turn into system-wide and the consequences can be catastrophic for an entire city, region or even a country.

In recent years, Russia has been actively conducting research in the field of cybersecurity of electric power systems (EPS). This is due to the increased frequency of cyber attacks on the EPS, the vulnerability of which has increased due to their intellectualization and digitalization, as a result of which the EPS have turned into cyber-physical systems in which the information and control subsystem is comparable in complexity and responsibility to the physical one.

Cyber threats arising as a result of the use of modern information technologies can be considered by the example of a multi-agent approach to systems that are open to large flows of heterogeneous data from heterogeneous sources and the possibility of connecting new types of agents, therefore they are fundamentally vulnerable from the point of view of cybersecurity, and new ways of ensuring its security and stability in relation to intentional cyber attacks. To do this, it must be protected against possible cyberattacks and be able to work effectively in conditions of receipt of extremely large data streams of different quality and reliability. Otherwise, a vulnerable control system will cause major man-made accidents. The analysis of system accidents indicates that the imperfection of control system algorithms increases the scale of consequences when local accidents turn into system-wide ones. So, since 2010, the number of detected vulnerabilities has increased 20 times, while every fifth vulnerability has been eliminated for longer than a month (Massel', Voropaj, Senderov, Massel', 2016).

An organization that is part of the AEC structure in the retail electricity market can be of a variety of activities, organizational structure, number and availability of trained personnel, cybersecurity requirements, which includes, among other things, the concept of information security and information technology security and apply to processes in the field of information technology, including cloud services, operation services, technical support, monitoring and maintenance of network infrastructure, computing systems, complexes and software provided to external and internal clients, which are provided by an effective combination of organizational, methodological measures and software and hardware.

In the field of power equipment of various organizations, there is excessive dependence on imports of many types of technologies, automated control systems and equipment management (sensors, controllers, microelectronics), software and various applications of foreign manufacturers, aggravated by the monopoly position of their suppliers. For example, for a large number of energy consumers, the main producers of the SCADA control and data collection system are foreign companies, which is also one of the threats to cybersecurity.

It should be noted that this hardware and software may not have been updated for a long time and may not meet modern cybersecurity requirements. Outdated software is an ideal target for hackers, so manufacturing companies should prepare their SCADA systems for potential cyber threats and external vulnerabilities.

In addition to outdated software, weaknesses can also be called the lack of secure remote access and regular configuration monitoring, the lack of access rights differentiation, control over the launch of various applications from the outside, and much more.

In the vast majority of cases, the cause of emerging cyber threats in modern conditions is not technology, but the human factor, which is often more important than the technical features of the attack. Many employees of organizations have the opportunity to work remotely and can use their personal phone for work purposes or access their company's email through personal devices. The vulnerabilities of users begin with their digital behavior - how they work and what they click on.

Smartphones are inherently personal, they contain valuable information about our activities, relationships, finances, likes and dislikes, increasingly blurring the line between personal and professional, which makes phones an attractive target for cyber attacks. Personal devices may not have the same level of protection as work devices, and employees have appropriate security training. Therefore, employees of companies should be regularly trained in the field of cybersecurity, taking into account all changes in the company's activities.

The smart grid can be briefly described as a computerized electric grid saturated with smart meters, which can provide benefits and services not only to end-users with their own microgeneration for dynamic pricing, but also for utilities, where smart meters not only collect information about electricity consumption, but also allow utilities to determine the habits of their end-users, up to the population when they are at home or not, when and what device turns on and off, even what TV program they watch (Greveler, Justus, Lohr, 2012).

Maintaining the confidentiality of end-users in an intelligent network is a research problem that has attracted considerable attention from the scientific community, and a number of protocols have already been proposed that increase confidentiality, for example, (Borges, Martucci, Muhlhauser, 2012; Li, Luo, 2012; Erkin, Troncoso-Pastoriza, Lagendijk, Perez-Gonzalez, 2013). A significant part of these protocols requires smart meters to interact with each other and with the utility

Currently, in Russia, on a legislative basis, the process of installing, first of all, millions of smart meters of domestic production in the population, which transmit information about electricity consumption to the management company and the electricity supplier. At the same time, disregard for privacy issues can lead to a violation of the right to privacy, citizens can become the object of manipulation, and public infrastructure can be threatened.

Many companies and organizations in Russia have already implemented or continue to implement solutions of domestic developers of energy forecasting and notification platforms for their own production of products, commercial and industrial buildings, using protocols of domestic developers to manage energy consumption in real time and actions to optimize their costs. New applications are emerging, for example, to detect overloads in old transformers or to monitor the reliability of various power equipment.

Smart meters are becoming ubiquitous, and the development of smart grids may face unprecedented threats. The development of digital platforms in connection with the active introduction of smart meters and the concept of intelligent energy systems for efficient energy supply to the end-user is significantly changing the cybersecurity landscape.

It is necessary to conduct comprehensive research and changes in the traditional approach to cybersecurity, develop advanced methods for detecting and mitigating cyber threats, algorithms for analyzing large amounts of data to detect malware, and introduce domestic solutions and intelligent network management platforms.

5 CONCLUSIONS

1. Today, due to the unstable geopolitical situation, the introduction of modern digital technologies and control systems makes the energy equipment of the end-user a convenient target for attacks by cybercriminals and may cause vulnerability of the AEC participant to foreign hackers and affect the reliability of the micro-energy system itself as a whole.

2. The topic of technological independence of domestic solutions has become one of the most important in the Russian market in recent years. Cyber threats pose a serious threat to the energy sector, which is why technical support companies are actively implementing new solutions to counter these threats.

3. The trend towards import substitution in key energy sectors of Russia has been actively developing in recent years, many state-owned enterprises and corporations are switching to domestic technologies and introducing modern import-independent Russian platforms for energy management. This also applies to cyberattack protection tools.

REFERENCES

Energeticheskaya strategiya Rossijskoj Federacii na period do 2035 goda. URL: https://minenergo.gov.ru/node/1026.

Stennikov, V.A., 2023. Ustojchivoe razvitie energetiki: tendencii i vyzovy. *Energeticheskaya politika*, № 2. pages 47-54.

Aktivnye energeticheskie kompleksy — pervyj shag k promyshlennym mikrogridam v Rossii. Ekspertno-analiticheskij doklad. M.: Infrastrukturnyj centr «Enerdzhinet», 2020.

Holkin, D., 2021. Arhitektura Interneta energii (IDEA). Versiya 2.0 2021. URL: https://idea-go.tech/IDEAwhitepaper-ru.pdf (data obrashcheniya 20.09.2023).

Hohlov, A., 2018. Raspredelennaya energetika v Rossii: potencial razvitiya. 2018. URL: https://energy.skolkovo.ru/downloads/documents/SEneC/Research/SKOLKOVO_EneC_DER-3.0_2018.02.01.pdf (data obrashcheniya 06.10.2023).

Suhov, A.A., Stushkina, N.A., 2021. Modernizaciya sistem elektrosnabzheniya sel'skih potrebitelej putem vnedreniya tekhnologij SmartGrid. *Mezhdunarodnyj tekhniko-ekonomicheskij zhurnal*,№ 5. pages 48-53.

Leshtaev, O.V., Stushkina, N.A., Zaginajlov, V.I., 2021. Analiz pokazatelej kachestva elektroenergii v sistemah elektrosnabzheniya s setevymi solnechnymi elektrostanciyami maloj moshchnosti. *Mezhdunarodnyj tekhniko-ekonomicheskij zhurnal*, № 5. pages 48-53.

IEC TR 62746-2: 2015 System interface between customer energy management system and the power management system. Edition 1.0 (2015 – 04).

IEC TR 63097: 2017 Smart Grid standardization roadmap. Edition 1.0 (2017-11-14).

Mishuchkov; V.I., Pushkareva, M.B., Belov, S.I., 2020. New Resources for Energy Audit and Energy Services in the Context of Developing Digital Technologies. 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon).

Voropaj, N.I., Kolosok, I.N., Korkina, E.S., Osak, A.B., 2019. Kiberugrozy i kiberbezopasnost' v elektroenergeticheskih sistemah. *Elektroenergetika glazami molodezhi-2019.* Materialy yubilejnoj H Mezhdunarodnoj nauchno-tekhnicheskoj konferencii. pages 32-37.

Massel', L.V., Voropaj, N.I., Senderov, S.M., Massel', A.T., 2016. Kiberbezopasnost' kak odna iz strategicheskih ugroz energeticheskoj bezopasnosti Rossii. *Voprosy kiberbezopasnosti,* 4. pages 2-10.

Greveler, U., Justus, B., Lohr, D., 2012. Multimedia content identification through smart meter power usage profiles. *in Computers, Privacy and Data Protection (CPDP 2012).*

Borges, F., Martucci, L. A., Muhlhauser, M., 2012. Analysis of Privacy-Enhancing protocols based on anonymity networks. *in Smart Grid Communications (SmartGridComm), 2012 IEEE Conference on, Tainan City, Taiwan.*

Li, F., Luo, B., 2012. Preserving data integrity for smart grid data aggregation. *In Smart grid communications (SmartGridComm), 2012 IEEE third international conference on,* pages 366–371.

Erkin, Z., Troncoso-Pastoriza, J.R., Lagendijk, R.L., Perez-Gonzalez, F., 2013. Privacy-preserving data aggregation in smart metering systems: an overview. *Signal processing magazine, IEEE,* 30(2):75–86.